



U.S. Department of Justice

Federal Bureau of Investigation

Washington, D.C. 20535

August 25, 2011

MR. ERIK LARSON



Subject: PTECH, INC.
FOIPA No. 1160974- 000

Dear Mr. Larson:

The enclosed documents were reviewed under the Freedom of Information/Privacy Acts (FOIPA), Title 5, United States Code, Section 552/552a. Deletions have been made to protect information which is exempt from disclosure, with the appropriate exemptions noted on the page next to the excision. In addition, a deleted page information sheet was inserted in the file to indicate where pages were withheld entirely. The exemptions used to withhold information are marked below and explained on the enclosed Form OPCA-16a:

Section 552

- ☒ (b)(1)
- ☐ (b)(2)
- ☐ (b)(3) _____
- _____
- _____
- _____
- ☐ (b)(4)
- ☐ (b)(5)
- ☒ (b)(6)

Section 552a

- ☒ (b)(7)(A)
- ☐ (b)(7)(B)
- ☒ (b)(7)(C)
- ☐ (b)(7)(D)
- ☐ (b)(7)(E)
- ☐ (b)(7)(F)
- ☐ (b)(8)
- ☐ (b)(9)
- ☐ (d)(5)
- ☐ (j)(2)
- ☐ (k)(1)
- ☐ (k)(2)
- ☐ (k)(3)
- ☐ (k)(4)
- ☐ (k)(5)
- ☐ (k)(6)
- ☐ (k)(7)

90 **page(s)** were reviewed and 62 **page(s)** are being released.

☒ Document(s) were located which originated with, or contained information concerning other Government agency(ies) [OGA]. This information has been:

☐ referred to the OGA for review and direct response to you.

☒ referred to the OGA for consultation. The FBI will correspond with you regarding this information when the consultation is finished.

☐ In accordance with standard FBI practice, this response neither confirms nor denies the existence of your subject's name on any watch lists.

☒ You have the right to appeal any denials in this release. Appeals should be directed in writing to the Director, Office of Information Policy, U.S. Department of Justice, 1425 New York Ave., NW, Suite 11050, Washington, D.C. 20530-0001. Your appeal must be received by OIP within sixty (60) days from the date of this letter in order to be considered timely. The envelope and the letter should be clearly marked "Freedom of Information Appeal." Please cite the FOIPA Number assigned to your request so that it may be easily identified.

☐ The enclosed material is from the main investigative file(s) in which the subject(s) of your request was the focus of the investigation. Our search located additional references, in files relating to other individuals, or matters, which may or may not be about your subject(s). Our experience has shown, when ident, references usually contain information similar to the information processed in the main file(s). Because of our significant backlog, we have given priority to processing only the main investigative file(s). If you want the references, you must submit a separate request for them in writing, and they will be reviewed at a later date, as time and resources permit.

☒ See additional information which follows.

Sincerely yours,



David M. Hardy
Section Chief
Record/Information
Dissemination Section
Records Management Division

Enclosure(s)

In response to your Freedom of Information Act (FOIA) request, enclosed is a processed copy of FBI Headquarters file 288B-HQ-1394667 and FBI Boston Field Office file 288B-BS-90939.

EXPLANATION OF EXEMPTIONS

SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552

- (b)(1) (A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified to such Executive order;
- (b)(2) related solely to the internal personnel rules and practices of an agency;
- (b)(3) specifically exempted from disclosure by statute (other than section 552b of this title), provided that such statute(A) requires that the matters be withheld from the public in such a manner as to leave no discretion on issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld;
- (b)(4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;
- (b)(5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;
- (b)(6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;
- (b)(7) records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information (A) could be reasonably be expected to interfere with enforcement proceedings, (B) would deprive a person of a right to a fair trial or an impartial adjudication, (C) could be reasonably expected to constitute an unwarranted invasion of personal privacy, (D) could reasonably be expected to disclose the identity of confidential source, including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of record or information compiled by a criminal law enforcement authority in the course of a criminal investigation, or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source, (E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or (F) could reasonably be expected to endanger the life or physical safety of any individual;
- (b)(8) contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions; or
- (b)(9) geological and geophysical information and data, including maps, concerning wells.

SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552a

- (d)(5) information compiled in reasonable anticipation of a civil action proceeding;
- (j)(2) material reporting investigative efforts pertaining to the enforcement of criminal law including efforts to prevent, control, or reduce crime or apprehend criminals;
- (k)(1) information which is currently and properly classified pursuant to an Executive order in the interest of the national defense or foreign policy, for example, information involving intelligence sources or methods;
- (k)(2) investigatory material compiled for law enforcement purposes, other than criminal, which did not result in loss of a right, benefit or privilege under Federal programs, or which would identify a source who furnished information pursuant to a promise that his/her identity would be held in confidence;
- (k)(3) material maintained in connection with providing protective services to the President of the United States or any other individual pursuant to the authority of Title 18, United States Code, Section 3056;
- (k)(4) required by statute to be maintained and used solely as statistical records;
- (k)(5) investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment or for access to classified information, the disclosure of which would reveal the identity of the person who furnished information pursuant to a promise that his/her identity would be held in confidence;
- (k)(6) testing or examination material used to determine individual qualifications for appointment or promotion in Federal Government service the release of which would compromise the testing or examination process;
- (k)(7) material used to determine potential for promotion in the armed services, the disclosure of which would reveal the identity of the person who furnished the material pursuant to a promise that his/her identity would be held in confidence.

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

Serial Description ~ COVER SHEET 08/24/2002

Total Deleted Page(s) ~ 28

Page 2 ~ Duplicate
Page 3 ~ Duplicate
Page 4 ~ Duplicate
Page 5 ~ Duplicate
Page 6 ~ Duplicate
Page 7 ~ Duplicate
Page 8 ~ Duplicate
Page 9 ~ Duplicate
Page 10 ~ Duplicate
Page 11 ~ Duplicate
Page 12 ~ Duplicate
Page 13 ~ Duplicate
Page 14 ~ Duplicate
Page 15 ~ Duplicate
Page 16 ~ Duplicate
Page 17 ~ Duplicate
Page 18 ~ Duplicate
Page 26 ~ Duplicate
Page 27 ~ Duplicate
Page 28 ~ Duplicate
Page 29 ~ Duplicate
Page 30 ~ Duplicate
Page 31 ~ Duplicate
Page 32 ~ Duplicate
Page 33 ~ Duplicate
Page 34 ~ Duplicate
Page 35 ~ Duplicate
Page 36 ~ Duplicate

XXXXXXXXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this Page X
XXXXXXXXXXXXXXXXXXXXXXXXXXXXX

(Rev. 01-31-2003)

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 09/3/2003

To: Boston

Attn: SSA [redacted] (CT-3)

SA [redacted] (CT-3)

SA [redacted]

SSA [redacted] (CT-1)

Counterterrorism

Attn: SSA [redacted]
CONUS II/ITOS 1, room 5270

SC [redacted]

TFOS, room 4871

Office of Public Affairs

Attn: SSA [redacted]
Congressional Affairs Office
Room 7240

b6
b7c

From: Cyber

CIS/C3IU/room 5931

Contact: SSA [redacted]

Approved By: [redacted]

Drafted By: [redacted] asm

Case ID #: (U) ~~(S)~~ [redacted]-CLASS (Pending)

b7A

(U) ~~(S)~~ 288B-BS-90939 (Closed)

~~(S)~~ 288B-HQ-1394667 (Closed)

(U) **Title:** ~~(S)~~ [redacted]

DBA, PTECH, INC.,
QUINCY, MASS.
AOT - IT - WCC

(U) **Synopsis:** ~~(S)~~ To provide receiving offices with (1) a copy of a White Paper regarding PTECH Inc., and (2) a letter addressed to Senator Charles Grassley, both prepared by Carnegie Mellon University CERT (computer incident response team).

(U) ~~(S)~~ **Derived From:** ~~G-3~~
Declassify On: ~~X1~~

(U) **Enclosures:** ~~(S)~~ Enclosed for receiving offices is one (1) copy of a document entitled, "White Paper: Possible Terrorist Links To Ptech, Inc., a U.S. Company", prepared by Carnegie Mellon CERT, and (2) copy of a letter addressed to Senator Grassley from Carnegie Mellon CERT (not dated).

~~SECRET~~

~~SECRET~~

To: Boston From: Cyber
(U) Re: ~~(S)~~ 265C-BS-90861-CLASS, 09/3/2003

Details: (U) Reference Boston EC to Counterterrorism dated 7/23/2003, and telcalls between SSA [] C3IU/CyD, SA [] Boston, and SSA [], ITOS/CTD.

(U) ~~(S)~~ For the information of receiving offices, on 8/12/2003, A/SC [] (U.S. Secret Service detailee to the Cyber Division, FBIHQ), Computer Intrusion Section (CIS), obtained the enclosed White Paper from the USSS congressional affairs office, Washington D.C. A/SC [] advised that the document was prepared by the CERT, Carnegie Mellon University, Pittsburgh, PA. pursuant to a request from Senator Charles Grassley's office thru USSS. He advised that CERT was requested to conduct technical analysis of Ptech software in connection with Senator Grassley's inquiries into the possible threat posed by Ptech and its product/services due to its alleged connections to terrorist groups and individuals. He advised that Senator Grassley's office staff may be requesting a meeting with the FBI once the CERT reports are completed and provided to the FBI for review.

b6
b7C

(U) ~~(S)~~ On 8/13/2003, through Cyber Division/CCIU and Pittsburgh Division liaison with Carnegie Mellon CERT, CERT provided a copy of a letter addressed to Senator Grassley from CERT. The letter was pursuant to Senator Grassley's request for the CERT to examine Ptech Inc. software for evidence of malicious code or "back doors." The letter also provided CERT's conclusions which in essence stated that the CERT's evaluation found no evidence of backdoors or other malicious code and that "further evaluation of the software will not yield new insights." CERT advise that the letter was forwarded

(U) In view of the above, C3IU/CyD will consider the referenced lead completed.

LEAD (S):

~~SECRET~~

~~SECRET~~

To: Boston From: Cyber
(U) Re: ~~(S)~~ 265C-BS-90861-CLASS, 09/3/2003

Set Lead 1: (Info)

BOSTON DIVISION

AT BOSTON, MASSACHUSETTS

(U) Read and clear.

Set Lead 2: (Info)

COUNTERTERRORISM

AT WASHINGTON D.C.

(U) Read and clear.

Set Lead 3: (Info)

OFFICE OF PUBLIC AFFAIRS

AT WASHINGTON D.C.

(U) Read and clear.

~~SECRET~~

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY

Date: 10/25/2002

To: CYBER

Attn: C3IU / CIS / #5931

SSA [REDACTED]
[REDACTED]

From: Boston

C-11

NIPC

Contact: SA [REDACTED]

b6
b7C

Approved By: [REDACTED]

Drafted By: [REDACTED]

klb

Case ID #: (U) 288B-BS-90939 (Pending)

(U) **Title:** ~~(S)~~ PTECH INC - SUBJECT (A U.S. COMPANY)
FBI, FAA, IRS, USAF, DOE, OTHER U.S.
GOVERNMENT AGENCIES - POSSIBLE VICTIMS
TARGETING THE NATIONAL INFORMATION
INFRASTRUCTURE - COUNTERINTELLIGENCE/
COUNTERTERRORISM (TNII-CI/CT)
OO:HQ

(S)

[REDACTED]
Investigative update to CYBER Division SSA [REDACTED]

b1

(U) ~~(S)~~

~~Derived From : G-3~~

~~Declassify On: X1~~

b6
b7C

(U) **Administrative:** ~~(S)~~ Reference telecall between SSA [REDACTED]
and SSA [REDACTED] SA [REDACTED] SA [REDACTED] on 10/25/2002.

(S)

b1

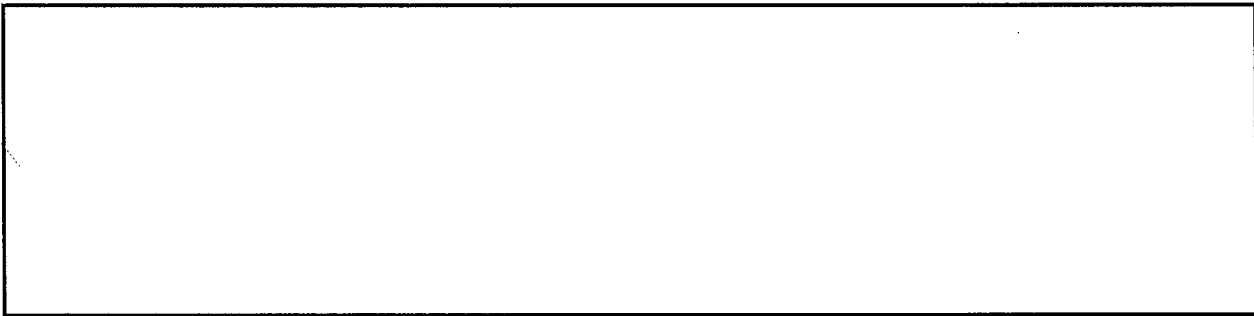
~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~SECRET~~

To: CYBER From: Boston
Re: (U) 288B-BS-90939, 10/25/2002

(S)



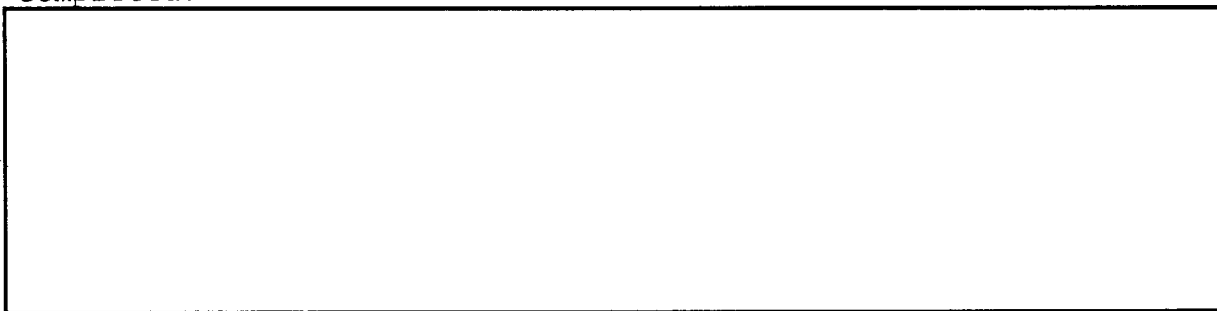
b1

(U)

~~(S)~~ Details: The following information is being provided as an investigate update to CYBER Division SSA [redacted] as of 10/25/2002. The following investigative actions have been completed:

b6
b7C

(S)



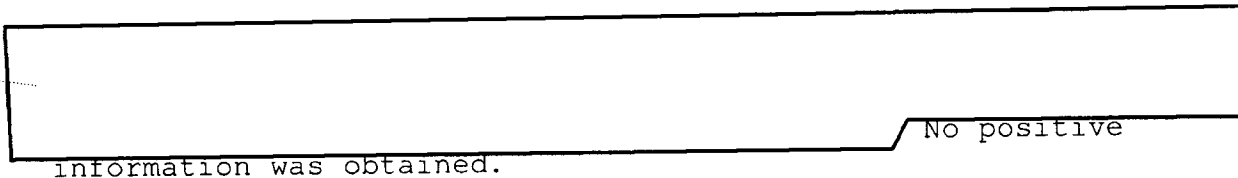
b1

(U)

~~(S)~~ SA [redacted] has interviewed both Boston Division Case Agents and Counterterrorism Supervisors responsible for the on-going parallel investigations. The case agent involved in 199N-BS-86457 and 199N-BS-86451 has received extensive NIPC training and is considered technically literate. No positive information was obtained.

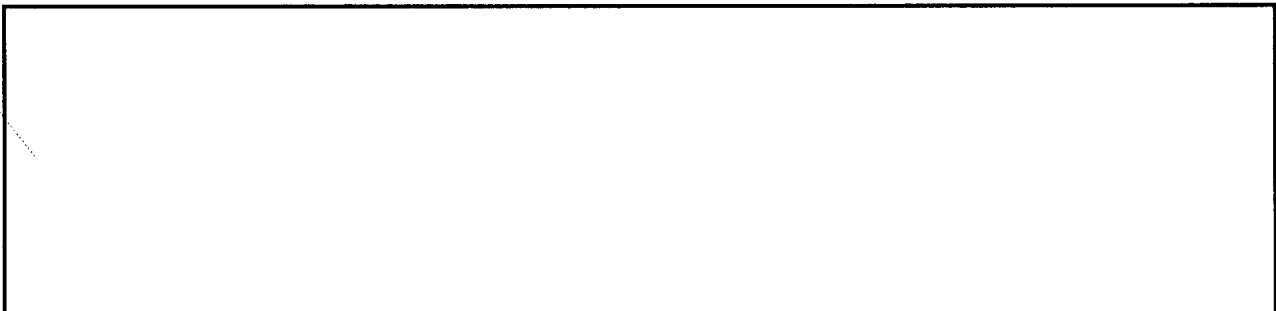
b6
b7C

(S)



information was obtained.

(S)



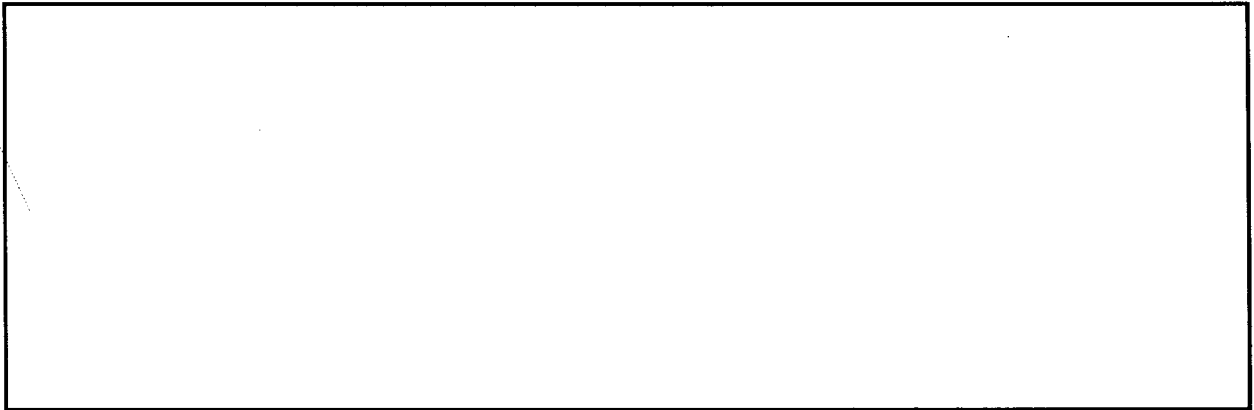
b1

~~SECRET~~

~~SECRET~~

To: CYBER From: Boston
Re: (U) 288B-BS-90939, 10/25/2002

(S)



b1

~~SECRET~~

~~SECRET~~

To: CYBER From: Boston
Re: (U) 288B-BS-90939, 10/25/2002

LEAD(s) :

Set Lead 1:

CYBER

AT WASHINGTON, DC

(S)

b1

♦♦

~~SECRET~~

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 10/30/2002

To: Counterterrorism

Attn: SSA [REDACTED]
UBLU, room 5448

b6
b7C

Boston

Attn: SSA [REDACTED]
Cyber Squad

Attn: SSA [REDACTED]
CT Squad

General Counsel

Attn: [REDACTED]
NSLU, room 7975

From: Cyber

CIS/C3IU

Contact: SSA [REDACTED]

Approved By: [REDACTED]

Drafted By: [REDACTED]

asm

(U) **Case ID #:** (S) 288B-HQ-1394667 (Pending)
(S) [REDACTED] (Pending)
(S) 288B-BS-90939 (Pending)

b7A

(U) **Title:** ~~(S)~~ PTECH INC. - SUBJECT (U.S. COMPANY);
FBI, FAA, IRS, USAF, DOE, OTHER U.S.
GOVERNMENT AGENCIES - POSSIBLE VICTIMS;
TARGETING THE NATIONAL INFORMATION
INFRASTRUCTURE - COUNTERINTELLIGENCE/
COUNTERTERRORISM (TNII-CI/CT)

Synopsis: ~~(S)~~ Submission of 90 day LHM for captioned USPER Full
Field Investigation (FI) due on 11/22/2002. [REDACTED]

b1

(U) ~~(S)~~ **Derived From:** G-3
Declassify On: X1

(U) **Full Field Investigation Instituted:** 08/23/2002

~~SECRET~~

~~SECRET~~

(U) To: Counterterrorism From: Cyber
Re: ~~(S)~~ 288B-HQ-1394667, 10/30/2002

(U) ~~(S)~~ **Enclosure(s):** ~~(S)~~ Original and one (1) copy of an LHM concerning status of captioned investigation to date.

(U) ~~(S)~~ **Details:** ~~(S)~~ Captioned FI was predicated on the Counterterrorism Division's (CTD) investigations of individuals with connections to international terrorism organizations and activities, and their connection to a computer software company named Ptech Inc., Boston, MA. One of the main focuses of the CT investigation is the individuals' association with organizations and business establishments suspected of funding terrorist groups and activities. Additionally, during 8/2002, it was determined that the FBI had acquired and was currently using a Ptech Inc. software product for use in connection with the FBI intranet system as a management tool.

(U) ~~(S)~~ The captioned TNII-CI/CT investigation was initiated for the purpose of determining Ptech's possible involvement in the planting of malicious or unauthorized code in their software thereby threatening the compromise of U.S. computer networks, including U.S. government computer systems. Ptech Inc. internet company web site has advertised their customer list to include the FBI, FAA, IRS, USAF, DOE and other government agencies. In view of the previous CTD ongoing investigations of individuals associated with Ptech Inc., the captioned TNII-CI/CT investigation initiated by the Cyber Division (C3IU) is in support of the CTD investigations, to primarily provide CTD with technical support and guidance.

(U) ~~(S)~~ In view of its supportive role to the CTD investigations, close coordination of parallel investigative efforts is being conducted at both the field and HQ levels. Additionally, the Boston Division CT and Cyber squads are coordinating their investigations of Ptech Inc. and the individuals associated with the company.

~~(S)~~ To date, preliminary technical analysis of the FBI purchased Ptech software and of computers loaded with the software, have not revealed any abnormalities or evidence of malicious or unauthorized code.

(S) reports, interviews, and other investigative results, have been negative for any evidence of Ptech Inc.'s involvement in the planting of malicious or unauthorized code in their software or otherwise engaging in activities that pose a threat to U.S. computer networks.

b1

~~SECRET~~

~~SECRET~~

To: Counterterrorism From: Cyber
(U) Re: ~~(S)~~ 288B-HQ-1394667, 10/30/2002

Referral/Consult

~~(S)~~

(S)

b1

(U)

Referral/Consult

~~SECRET~~

~~SECRET~~

To: Counterterrorism From: Cyber
(U) Re: ~~(S)~~ 288B-HQ-1394667, 10/30/2002

LEAD(s) :

Set Lead 1:

BOSTON

AT BOSTON, MASSACHUSETTS

(U) Read and clear.

Set Lead 2:

COUNTERTERRORISM

AT WASHINGTON, DC

USAMA BIN LADEN UNIT (UBLU)

(U) Read and clear.

Set Lead 3:

GENERAL COUNSEL

AT WASHINGTON, DC

(S)

×

b1

♦♦

~~SECRET~~

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 11/07/2002

To: Counterterrorism

Attn: SSA [REDACTED]
UBLU, room 5448

Cyber

Attn: SSA [REDACTED]
CIS/C3IU

Boston

Attn: SSA [REDACTED]
CT-1 [REDACTED]
SSA [REDACTED]
CT-3 [REDACTED]
SA [REDACTED]
CT-3 [REDACTED]
SA [REDACTED]
CT-1 [REDACTED]
SA [REDACTED]
C-11 [REDACTED]

b6
b7C

General Counsel

Attn: [REDACTED]
NSLU, room 7975

From: Boston
C-11

Contact: CSFE [REDACTED]

Approved By: [REDACTED]

Drafted By: [REDACTED] ss

Case ID #: (S) 288B-BS-90939 (Pending)
(S) [REDACTED] (Pending)
(U) (S) 288B-BS-90939 (Pending)
(S) 199N-BS-86451 (Pending)
(S) 199N-BS-86457 (Pending)
(S) 288B-HQ-1394667 (Pending)

b7A

(U) **Title:** ~~(S)~~ PTECH INC. -SUBJECT (U.S. COMPANY);
FBI, FAA, IRS, USAF, DOE, OTHER U.S.
GOVERNMENT AGENCIES - POSSIBLE VICTIMS;
TARGETING THE NATIONAL INFORMATION
INFRASTRUCTURE - COUNTERINTELLIGENCE/
COUNTERTERRORISM (TNII-CI/CT)

~~SECRET~~

~~SECRET~~

(U) To: Counterterrorism
Re: ~~S~~ 288B-BS-90939

From: Boston
11/07/2002

(S)

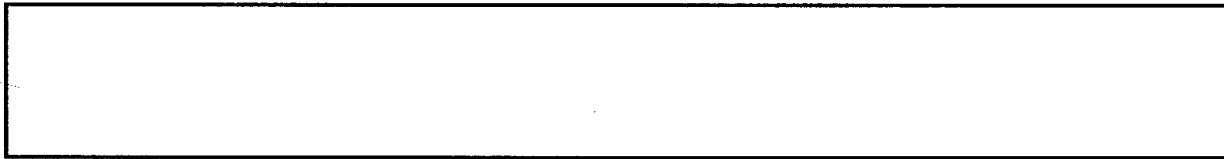


(U) ~~S~~

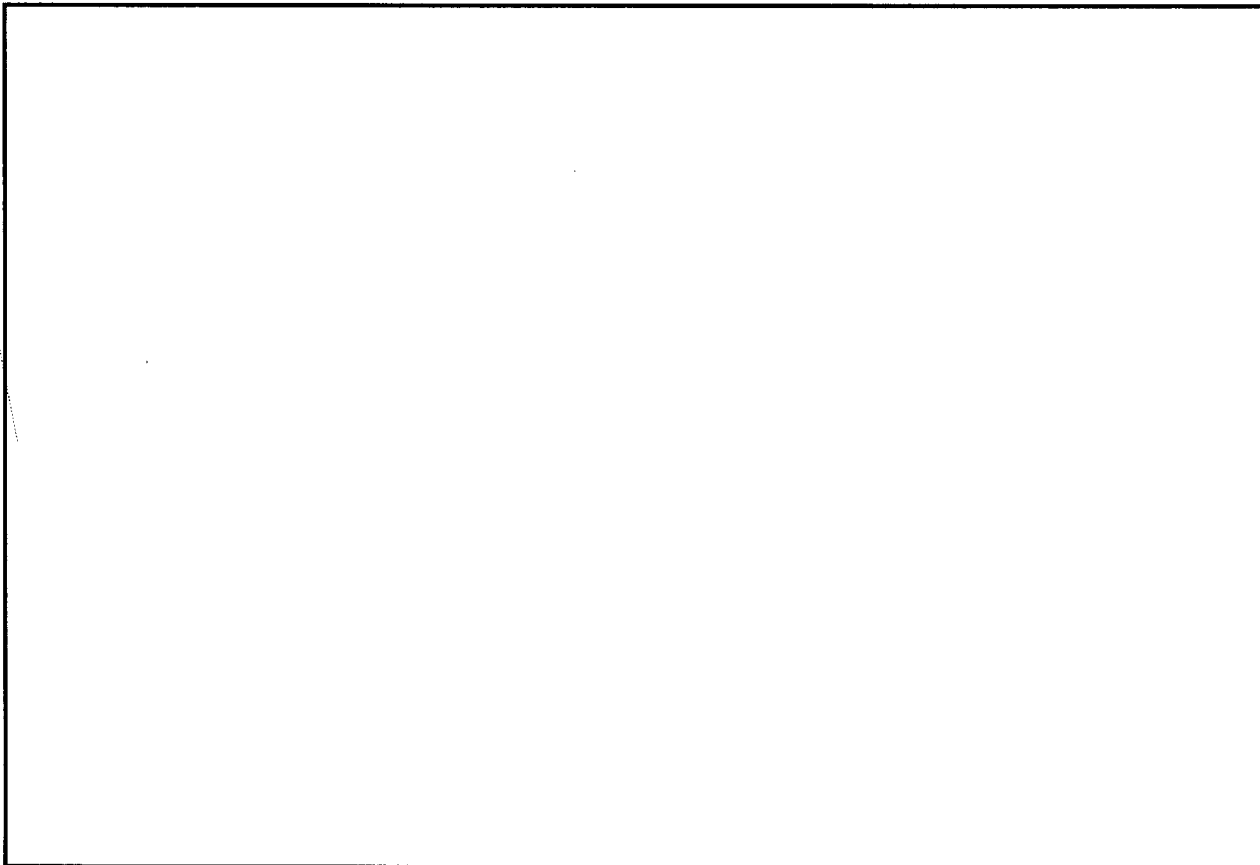
Derived From : ~~G-3~~
Declassify On: ~~X1~~

(U) Full Field Investigation Instituted: 08/23/2002

(S)



(S)



b1

~~SECRET~~

~~SECRET~~

(U) To: Counterterrorism
Re: ~~(S)~~ 288B-BS-90939

From: Boston
11/07/2002

(S)

b1

~~SECRET~~

~~SECRET~~

To: Counterterrorism
(U) Re: ~~(S)~~ 288B-BS-90939

From: Boston
11/07/2002

(S)

b1

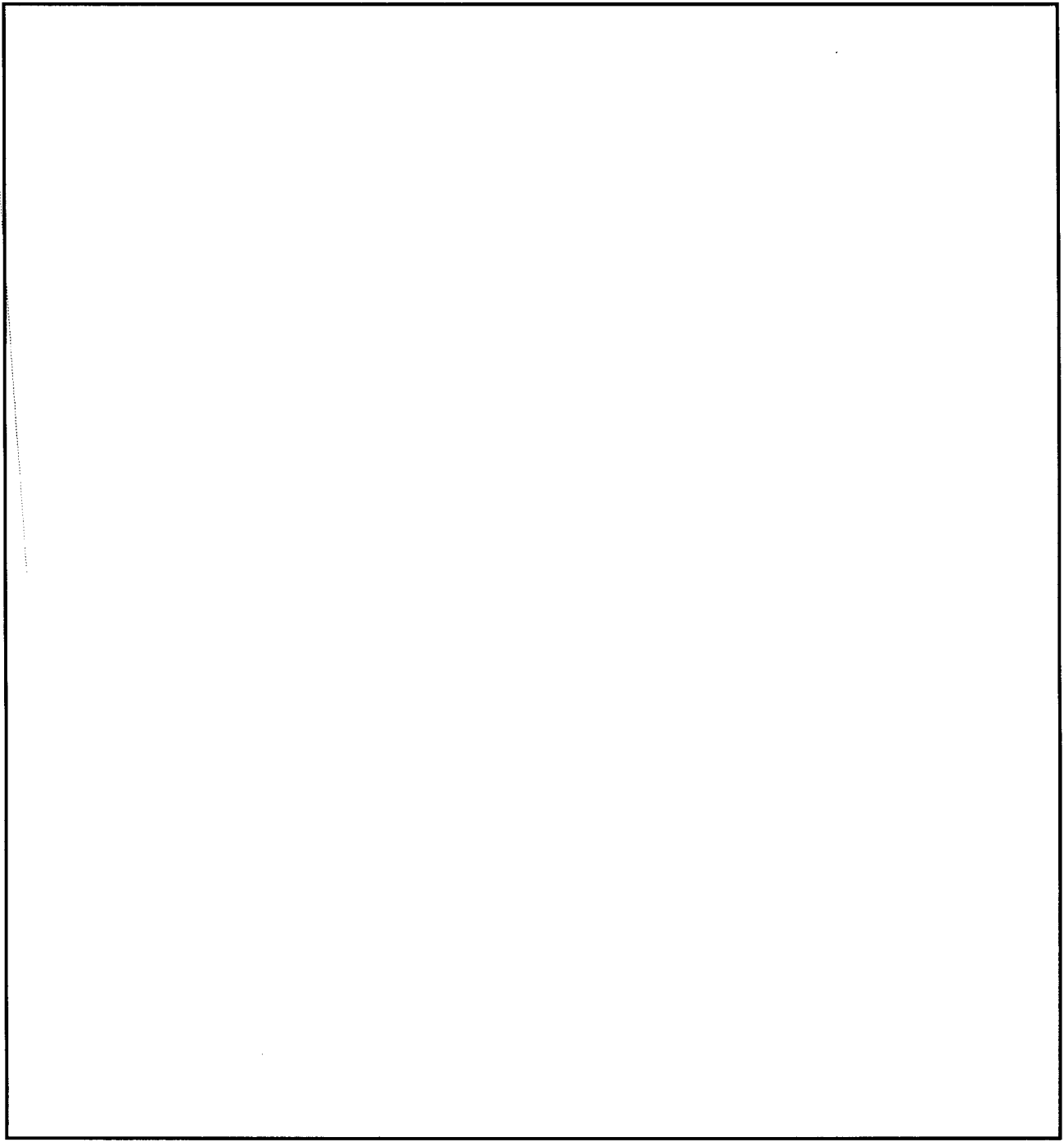
~~SECRET~~

~~SECRET~~

(U) To: Counterterrorism
Re: ~~(S)~~ 288B-BS-90939

From: Boston
11/07/2002

(S)



b1

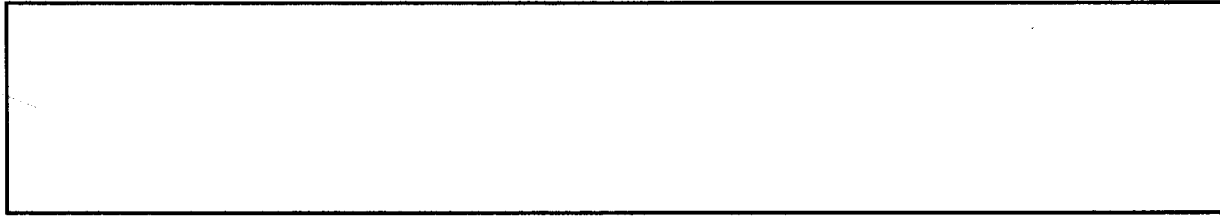
~~SECRET~~

~~SECRET~~

To: Counterterrorism
(U) Re: ~~(S)~~ 288B-BS-90939

From: Boston
11/07/2002

(S)



b1

~~SECRET~~

~~SECRET~~

To: Counterterrorism
(U) Re: ~~(S)~~ 288B-BS-90939

From: Boston
11/07/2002

LEAD(s):

Set Lead 1:

BOSTON

AT BOSTON, MASSACHUSETTS

(U) Read and clear.

Set Lead 2:

COUNTERTERRORISM

AT WASHINGTON, DC

USAMA BIN LADEN UNIT (UBLU)

(U) Read and clear.

Set Lead 3:

CYBER

AT WASHINGTON, DC

CIS/C3IU

(U) Read and clear.

♦♦

~~SECRET~~

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 11/15/2002

To: Cyber
Boston

Attn:

CIS/C3IU

SSA

CT-1

SSA

CT-3

SA

CT-3

SA

CT-1

SSA

UBLU, room 5448

Counterterrorism

From: Boston
C-11

Contact:

Approved By:

Drafted By:

sj0

(U) **Case ID #:** ~~(S)~~ 288B-BS-90939 (Pending)

(U) **Title:** ~~(S)~~ PTECH INC. -SUBJECT (U.S.COMPANY);
FBI, FAA, IRS, USAF, DOE, OTHER U.S.
GOVERNMENT AGENCIES - POSSIBLE VICTIMS;
TARGETING THE NATIONAL INFORMATION
INFRASTRUCTURE - COUNTERINTELLIGENCE/
COUNTERTERRORISM (TNII-CI/CT)

(U) **Synopsis:** ~~(S)~~ To report current investigative action by case
agent

(U) ~~(S)~~

~~Derived From : G-3~~
~~Declassify On: X1~~

(S)

b1

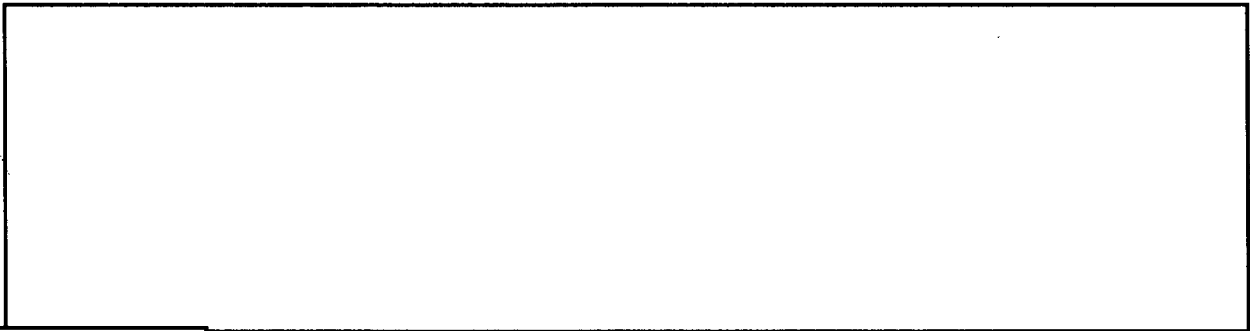
~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~SECRET~~

To: Cyber From: Boston
(U) Re: ~~(S)~~ 288B-BS-90939, 11/15/2002

(S)



b1

 The examination revealed no evidence of the presence of any malicious code on Ptech's software.

~~SECRET~~

~~SECRET~~

(U) To: Cyber From: Boston
Re: ~~(S)~~ 288B-BS-90939, 11/15/2002

LEAD(s) :

Set Lead 1:

BOSTON

AT BOSTON, MASSACHUSETTS

(U) Read and clear.

Set Lead 2:

COUNTERTERRORISM

AT WASHINGTON, DC

(U) Read and clear.

Set Lead 3:

CYBER

AT WASHINGTON, DC

CIS/C3IU

(U) Read and clear.

♦♦

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 12/12/2002

To: Boston

From: Boston

Hudson RA

Contact: SA [REDACTED]

Approved By: [REDACTED]

b6
b7C

Drafted By: [REDACTED] jat

Case ID #: 288B-BS-90939 (Pending)
199N-BS-77139 (Pending)

Title: P-TECH

Synopsis: On 12/12/2002, an anonymous telephone call was received from a female providing information about P-TECH.

Details: On 12/12/2002, an anonymous female contacted the Hudson RA from a phone booth. She refused to identify herself. She stated the information was from personal knowledge.

[REDACTED] She stated [REDACTED] of Canton, MA, telephone [REDACTED] was [REDACTED] at P-TECH in 2000.

She believes [REDACTED] was associated with [REDACTED] of HEALY HUDSON of 101 Federal Street. [REDACTED] was [REDACTED] and [REDACTED] was an employee. HEALY HUDSON went out of business in June 2002.

[REDACTED] [REDACTED] of WINCHESTER, MA, telephone [REDACTED] now of OCCHSLE INTERNATIONAL ADVISORS, Boston, MA may also have worked at HEALY HUDSON.

She believed this information would be helpful to those investigating P-TECH.

She refused to identify herself and provided no recontact number.

♦♦

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 01/02/2003

To: Boston

Attn: SA [REDACTED]

CYBER

Squad C-11

SSA [REDACTED]

b6
b7C

From: CYBER

STAS/TAU/Room 5931

Contact: SSA [REDACTED]

Approved By: [REDACTED]

Drafted By: [REDACTED]

tbf

Case ID #: (U) 288B-BS-90939 (Pending)
(U) 66F-HQ-C1319773 (None)

(U) **Title:** ~~(S)~~ PTECH INC. - SUBJECT (A U.S. COMPANY)
FBI, FAA, IRS, USAF, DOE, OTHER U.S.
GOVERNMENT AGENCIES - POSSIBLE VICTIMS
TARGETING THE NATIONAL INFORMATION
INFRASTRUCTURE- COUNTERINTELLIGENCE/
COUNTERTERRORISM (TNII-CI/CT)
OO:HQ

(S)

(U) ~~(S)~~

~~Derived From : G-3~~
~~Declassify On: X1~~

b1

(S)

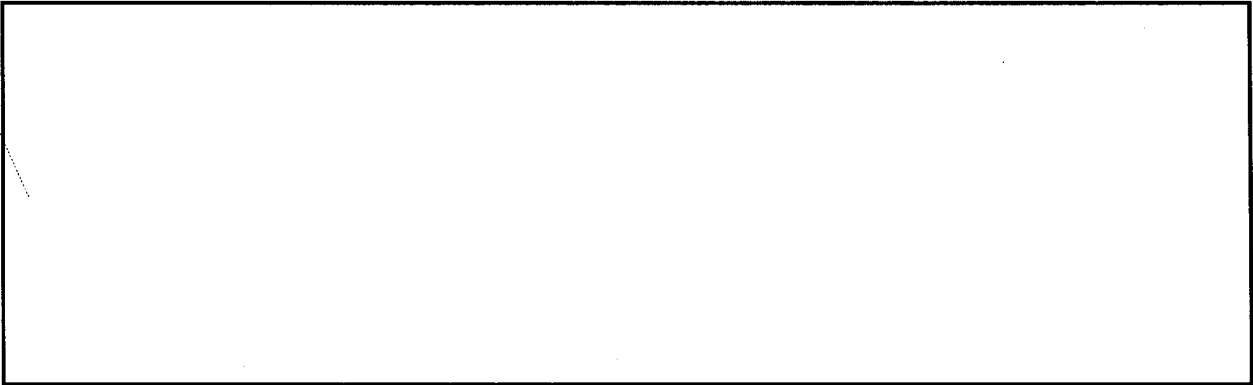
~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~SECRET~~

To: Boston From: CYBER
Re: (U) 288B-BS-90939, 01/02/2003

(S)



b1

♦♦

~~SECRET~~



U.S. Department of Justice

Federal Bureau of Investigation

DATE: 06-23-2011

Washington, D. C. 20535-0001

FBI INFO.

CLASSIFIED BY 60324 UCBAW/SAB/SBS

REASON: 1.4 (c)

DECLASSIFY ON: 06-23-2036

April 2, 2003

(U) ~~(S)~~ PTECH INC. - SUBJECT (U.S. COMPANY);
FBI, FAA, IRS, USAF, DOE, OTHER U.S. GOVERNMENT AGENCIES -
POSSIBLE VICTIMS;
TARGETING THE NATIONAL INFORMATION INFRASTRUCTURE -
COUNTERINTELLIGENCE/COUNTERTERRORISM (TNII-CI/CT)
FILE #288B-HQ-1394667

(U) Full Field Investigation instituted: 8/23/2002

(U) ~~(S)~~ Derived From: G-3
Declassify On: X-1

(U) ~~(S)~~ Since June 1995, the Boston FBI Counterterrorism
(CT) squads have been investigating several individuals who have
had numerous contacts and associations with persons and groups
suspected of ties to international terrorism. Some of these
individuals include [REDACTED]

[REDACTED] are associated, as described below,
with Ptech Inc. (Ptech), Quincy, Massachusetts, a computer
software company. Source reporting and the Ptech Internet
website have listed the FBI, FAA, IRS, USAF, DOE, and other U.S.
government agencies as Ptech customers. Source information has
also reported that Ptech may have done business with the White
House and/or the Vice President's office, under the auspices of
another company named Process Renewal Group (PRG).

(U) ~~(S)~~ Ptech Inc. is a business involved in providing
enterprise architecture and business modeling, analysis and
integration solutions to Global 2000 companies. This technology
addresses every aspect of the organization, from strategic
planning, to business architecture; from business processes to
network, supporting applications, and all forms of information,
which is integrated to form a complete representation of the
company's knowledge. Massachusetts State corporate records list
Ptech Inc. as a partnership, its business address as 160 Federal
Street, Boston, MA. 02110, and its [REDACTED] as
[REDACTED]. The
records further references an involuntary dissolution date of
8/31/1998, and a subsequent revival date of 6/1/2001.
Lexis/Nexis checks of Ptech list the company's other principals

b6
b7c

~~SECRET/NOFORN/ORCON~~

as [redacted]

and [redacted]

b6
b7C

(U) ~~(S)~~ On 6/27/1995, FBI Boston opened a preliminary inquiry (PI) on [redacted] based on his telephone contacts with the Holy Land Foundation for Relief and Development (HLFRD), Dallas, Texas. HLFRD is an organization suspected of being a source for funding terrorist activities and groups.

(U) ~~(S/NF/OC)~~ Investigation of [redacted] had also revealed that he had telephone contacts with [redacted] subjects and was associated with other Boston international terrorism subjects. A Full Field Investigation (FFI) (199N-BS-77139) was initiated by FBI Boston on 6/11/2002.

(U) ~~(S)~~ Source information has indicated that [redacted] and other Ptech employees traveled to Saudi Arabia, during February 1999, to seek funding from a wealthy Saudi Arabian name [redacted]. Sources have also reported that [redacted] may have been the source of approximately \$16 million in startup funds for Ptech. [redacted] has been described as one of the "chief money launderers" for OSAMA BIN LADEN.

(U) ~~(S)~~ Source reporting has indicated that another individual, [redacted] is associated with [redacted] and Ptech. [redacted] is reported to be a Pakistani National on the Ptech Board of Directors. [redacted] is also the head of SAAR Foundation, Herndon, VA. This foundation has been linked to financial organizations that are being investigated for handling large sums of money to fund activities for OSAMA BIN LADEN and various other terrorist organizations. SAAR is the subject of a U.S. Customs Service (USCS)/Joint Terrorism Task Force (JTTF) case. [redacted] is a central figure in this investigation. Searches of the offices of SAAR Foundation, and other foundations in the Northern Virginia area, were conducted by federal agents during March 2002, in connection with the USCS/JTTF investigation.

~~(S/NF/OC)~~ [redacted] a U.S. person, is employed as a computer software engineer for Ptech. [redacted] also serves as the current president and as a long-time member of CARE INTERNATIONAL, a non-governmental organization in Boston with ties to international terrorism and as a source of funding for terrorist activities. [redacted] is the subject of a FBI Boston FFI (199N-BS-86457).

(S) [redacted] This investigation has revealed that CARE INTERNATIONAL serves as a front for recruiting local Muslims to participate in international jihad effort.

b1

~~SECRET/NOFORN/ORCON~~

~~SECRET/NOFORN/ORCON~~

b6
b7c

(U) ~~(S/NF/OC)~~ [redacted] is an employee of Ptech Inc., in Boston, and is the [redacted] of Care International, a non-governmental organization in Boston with ties to international terrorism. Care International was previously known as the Al-Kifah Refugee Center of Boston. Following the World Trade Center attack in 1993, Al-Kifah changed its name to Care International after the media reported that members of the Al-Kifah Refugee Center of New York were involved in the attack. In the Boston area, Care International has served as a front for recruiting/funding local Muslims to participate in the international Jihad efforts. [redacted] is closely associated with [redacted] of Care International.

(U) ~~(S)~~ On May 28, 2002, a complainant working for JP Morgan Chase in Manhattan, NY, reported suspicious business practices by Ptech. This complainant was concerned that Ptech was involved in the theft of technology from U.S. companies. This complainant advised that [redacted] is connected to organizations which provide funding for terrorist purposes. This complainant further indicated that a Ptech employee may have tried to gain access to the Chase network during a demonstration of Ptech products and/or services, although there is no independent information to corroborate this.

(U) ~~(S)~~ On August 23, 2002, it was determined that the Information Resources Management (IRM) Office, FBIHQ, had purchased Enterprise Architecture computer software from Ptech in early 2001. This software, named "Framework," was being used as a management tool for the FBI's intranet network and is used for the FBI Enterprise Architecture project. The software allows users to access the FBI's Strategic Plan, organization chart, business processes, and other applications.

(U) ~~(S)~~ Ptech Framework software originals and copies including updated versions and "accelerators" were provided to the Counterintelligence Counterterrorism Computer Intrusion Unit (C3IU), Cyber Division, by IRM for technical analysis. Technical analysis of the Ptech software by the Special Technologies and Applications Section (STAS) to date has not revealed any evidence of malicious (eg. trojans, backdoors, viruses, worms, etc.) or any other unauthorized code imbedded in the software. Examination of two IRM computers used to run the software has not revealed any abnormalities. According to IRM, the Ptech software was not used to connect to the FBI computer network.

(S) [redacted]
[redacted]

~~SECRET/NOFORN/ORCON~~

Referral/Consult

~~SECRET/NOFORN/ORCON~~

Referral/Consult

- (U) ~~(S)~~ IRM personnel (section chief, chief architect, computer scientist, contractors) who worked with the Ptech software on the FBI Enterprise Architecture project have been interviewed. These individuals had no direct contacts or dealings with Ptech or its personnel with the exception of receiving training from instructors from Ptech. The reason is that the Ptech software purchased by the FBI was actually purchased through a government contractor called SPAWAR (Space and Naval Warfare). The interviews did not indicate any unusual or suspicious activity on the part of Ptech or of the performance and operation of the Ptech software used by the FBI.
- (U) ~~(S)~~ C3IU has obtained documents from IRM and the Contracts Unit that relate to the FBI purchase of the Ptech software. The documents indicate that during 12/2001, the FBI purchased two licensed copies of the Ptech Framework software, including updates and accelerators, for use in developing the FBI's Enterprise Architecture (EA) at a cost of \$15,000. The purchase was actually made by SPAWAR on behalf of the FBI and pursuant to the SPAWAR contract.
- (U) ~~(S)~~ The FBI New York Cyber squad has advised that they worked with the security department of JP Morgan Chase Bank, NY, concerning Ptech's efforts to market their software to the bank. JP Morgan security advised that a Ptech representative was allowed limited access to the company's network for this purpose. JP Morgan Chase Bank security conducted a thorough search of all areas of their network accessed by the Ptech representative but did not find any abnormalities. They advised that during a Ptech software demonstration at JP Morgan Bank, JP Morgan denied the Ptech's representative's request to connect his computer with the company's network. As a result of the above dealings with Ptech, JP Morgan did not purchase software from the company.
- (U) ~~(S)~~ Source information and public records have indicated that the Process Renewal Group (PRG) is a consulting group out of Vancouver, British Columbia, Canada. A former Ptech Inc. employee, [redacted] was once employed by PRG. Source information has further indicated that PRG never had a contract with the White House as has been claimed by Ptech advertisements and is believed to be fabricated by [redacted] and others for the benefit of Ptech. The Contracts Unit, Finance Division, FBIHQ, advised that they failed to locate any records of doing business with PRG.

b6
b7C

~~SECRET/NOFORN/ORCON~~

~~SECRET/NOFORN/ORCON~~

(S) to date, ~~(S)~~ The FBI Boston's counterterrorism investigation developed any information or indications that Ptech has been involved in the installation of any malicious or unauthorized code or backdoors into the FBI or other government networks, either through their software or services. b1

(U) ~~(S)~~ The FBI Boston Division Cyber squad has been working closely with the Boston Counterterrorism squads to coordinate the investigations of Ptech and its principals. Boston's Cyber squad in conjunction with FBIHQ, has been coordinating their efforts to evaluate the extent and nature of the threat to the national information infrastructure posed by Ptech Inc., its products/services, and its principals and employees.

(S)

(S)

b1

positive information was obtained.

NO

(S)

No positive information was obtained.

(U)

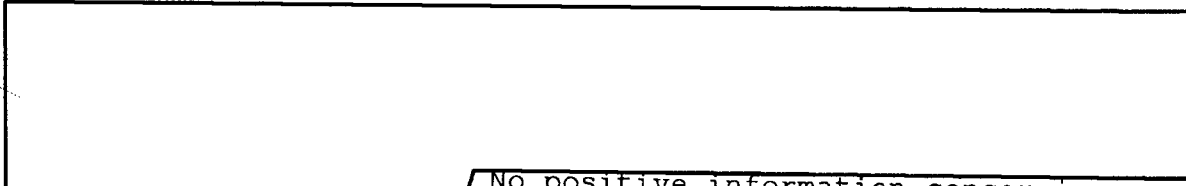
~~(S)~~ IRM conducted a canvass of all FBI divisions to determine if any other Ptech products were being used or had been acquired. The results of the canvass determined that no one else in the FBI reported acquiring or using any Ptech products. IRM and the FBI has discontinued the use of the Ptech Framework

~~SECRET/NOFORN/ORCON~~

~~SECRET/NOFORN/ORCON~~

software and a decision has been made not to acquire or use Ptech products in the future.

(S)



b1

No positive information concerning Ptech's possible implantation of malicious or unauthorized code in their software was discovered.

(U)

~~(S)~~ During November 2002, FBI Boston received source information concerning the source's knowledge of Ptech's business and products, and Ptech [redacted]. The source advised that Ptech products are stand alone products, that is not designed or meant to interface or operate directly on or with a customer's company network. According to the source, [redacted] resisted putting the capabilities in the Ptech software that would allow it to interface with other software running on the customer's computer network. The source stated that the Ptech software was not designed with hidden bugs or viruses, nor could it be manipulated remotely by someone. In the opinion of the source, any such manipulation of the Ptech products would be obvious to and immediately rejected by its customers or users.

b6
b7C

(S)



b1

(U)

~~(S)~~ Recently, the U.S. Customs Service conducted a highly publicized search of the Ptech offices in Boston, in connection with their terrorist related investigation of Ptech and some of its principles. The FBI has not received any information resulting from the Custom's search and Ptech investigation indicating any specific threat to the national security and critical infrastructures, posed by Ptech software and/or services.

(U) The FBI has not received any information from any Ptech customers, any federal agency or anyone else, concerning a report of a specific threat or actual anomalous behavior

~~SECRET/NOFORN/ORCON~~

~~SECRET~~/NOFORN/ORCON

exhibited or detected resulting from the use of Ptech software or services.

(U) Absent any specific information indicating a specific threat to the national security and U.S. information infrastructure posed by Ptech software and/or services, its principles and employees, no further investigation is warranted by the FBI.

~~SECRET~~/NOFORN/ORCON

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 04/04/2003

To: Counterterrorism

Attn: SSA [REDACTED]

IOS [REDACTED]

Boston

ITOS-1/Conus II. room 5432

Attn: SSA [REDACTED]

Cyber Squad

Attn: SSA [REDACTED]

CT Squad

General Counsel

Attn: [REDACTED]

NSLU, room 7975

b6
b7C

From: Cyber

CIS/C3IU/room 5931

Contact: SSA [REDACTED]

Approved By: [REDACTED]

Drafted By: [REDACTED]

asm

Case ID #: (S) 288B-HQ-1394667 (Closed)
(U) (S) 265C-BS-90861 (Pending)
(S) 288B-BS-90939 (Pending)

(U) **Title:** (S) PTECH INC. - SUBJECT (U.S. COMPANY);
FBI, FAA, IRS, USAF, DOE, OTHER U.S.
GOVERNMENT AGENCIES - POSSIBLE VICTIMS;
TARGETING THE NATIONAL INFORMATION
INFRASTRUCTURE - COUNTERTERRORISM/
COUNTERINTELLIGENCE (TNII-CT/CI)

Synopsis: (S) Submission of closing LHM for captioned USPER
Full Field Investigation (FFI). [REDACTED]

b1

(S)

(U) (S)

~~Derived From: G-3~~
~~Declassify On: X1~~

(U) Full Field Investigation Instituted: 08/23/2002

~~SECRET~~

~~SECRET~~

To: Counterterrorism From: Cyber
(U) Re: ~~(S)~~ 288B-HQ-1394667, 04/04/2003

(U) ~~(S)~~ **Enclosure(s):** ~~(S)~~ Original and one (1) copy of an LHM concerning the status and basis for closing captioned case.

(U) ~~(S)~~ **Details:** ~~(S)~~ Captioned FFI was predicated on the Counterterrorism Division's (CTD) investigations of individuals with connections to international terrorism organizations and activities, and their connection to a computer software company named Ptech Inc., Boston, MA. One of the main focuses of the CT investigation is the individuals' association with organizations and business establishments suspected of funding terrorist groups and activities. Additionally, during 8/2002, it was determined that the FBI had acquired and was currently using a Ptech Inc. software product for use in connection with the FBI intranet system as a management tool.

(U) ~~(S)~~ The captioned TNII-CI/CT investigation was initiated for the purpose of determining Ptech's possible involvement in the planting of malicious or unauthorized code in their software thereby threatening the possible compromise of U.S. computer networks, including vital U.S. government computer systems. Ptech Inc. Internet company web site has advertised their customer list to include the FBI, FAA, IRS, USAF, DOE and other government agencies. The captioned TNII-CI/CT investigation initiated by the Cyber Division (C3IU) is in support of the CTD investigations relating to Ptech, to primarily provide CTD with technical support and guidance, and to fully investigate and assess the potential threat to the U.S. information infrastructure, if any, posed by Ptech, its products/services, and its principals and employees.

(U) ~~(S)~~ In view of its supportive role to the CTD investigations, close coordination of parallel investigative efforts was being conducted at both the field and HQ levels. Additionally, the Boston Division CT and Cyber squads are coordinating their investigations of Ptech Inc. and the individuals associated with the company.

~~(S)~~ To date, prophylactic technical analysis of the FBI purchased Ptech software and of computers loaded with the software, have not revealed indicia of any abnormalities or evidence of malicious or unauthorized code. [REDACTED]

(S) [REDACTED] reports, interviews, source reporting and other investigative results, have been negative for any evidence of Ptech Inc.'s involvement in the planting of malicious or unauthorized code in their software or otherwise

b1

~~SECRET~~

~~SECRET~~

(U) To: Counterterrorism From: Cyber
Re: ~~SI~~ 288B-HQ-1394667, 04/04/2003

engaging in activities that pose a threat to U.S. computer networks.

(S) [REDACTED]

Referral/Consult

(U) In view of the above, CyD will discontinue any further investigation of the TNII-CT/CI matter, absent any indication of a specific threat posed by Ptech or its products and services to the U.S. information infrastructure. CyD will continue its technical support of the continuing CT investigation concerning individuals associated with Ptech.

~~SECRET~~

~~SECRET~~

(U) To: Counterterrorism From: Cyber
Re: ~~(S)~~ 288B-HQ-1394667, 04/04/2003

LEAD(s) :

Set Lead 1: (Discretionary)

BOSTON

AT AT BOSTON, MASSACHUSETTS

(U) For Boston Cyber Squad. C3IU recommends Boston close their parallel TNII-CT/CI matter when appropriate, in view of the closing of the FBIHQ case.

Set Lead 2: (Info)

COUNTERTERRORISM

AT AT WASHINGTON D.C.

(U) For ITOS-1/Conus II. Read and clear.

Set Lead 3: (Action)

GENERAL COUNSEL

AT WASHINGTON, DC

(S)

×

b1

♦♦

~~SECRET~~

~~SECRET/NOFORN/ORCON~~

DATE: 06-23-2011
CLASSIFIED BY 60324 UCBAW/SAB/SBS
REASON: 1.4 (c)
DECLASSIFY ON: 06-23-2036



U.S. Department of Justice

Federal Bureau of Investigation

In Reply, Please Refer to
File No.

Boston, MA 02108
March 11, 2003

(U) ~~(S)~~ PTECH INC. - SUBJECT (U.S. COMPANY);
FBI, FAA, IRS, USAF, DOE, OTHER U.S. GOVERNMENT AGENCIES -
POSSIBLE VICTIMS;
TARGETING THE NATIONAL INFORMATION INFRASTRUCTURE -
COUNTERINTELLIGENCE/COUNTERTERRORISM (TNII-CI/CT)
FILE #288B-BS-90939

(U) Full Field Investigation instituted: 9/12/2002

(U) ~~(S)~~ ~~Derived From: G-3~~
~~Declassify On: X-1~~

b1

(S)

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~SECRET/NOFORN/ORCON~~

~~SECRET~~/NOFORN/ORCON

(S)

b1

No positive information was obtained.

(U) Investigation completed. No further investigation
is warranted

~~SECRET/ORCON/NOFORN~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 4/11/2003

To: Cyber
Boston

Attn:

CIS/C310

SSA

CT-1

SSA

CT-3

SA

CT-1

SA

CT-1

General Counsel

NSLU, room 7975

b6
b7C

From: Boston

C-11

Contact:

Approved By:

Drafted By:

sj0

(U) **Case ID #:** ~~(S)~~ 288B-BS-90939 (Pending)

(U) **Title:** ~~(S)~~ PTECH INC. -SUBJECT (U.S.COMPANY);
FBI, FAA, IRS, USAF, DOE, OTHER U.S.
GOVERNMENT AGENCIES - POSSIBLE VICTIMS;
TARGETING THE NATIONAL INFORMATION
INFRASTRUCTURE - COUNTERINTELLIGENCE/
COUNTER TERRORISM (TNII-CI/CT)

(U) **Synopsis:** ~~(S)~~ Submission of closing LHM for captioned Full
Field Investigation (FI) and request to close above captioned
case.

(U) ~~(S)~~

~~Derived From: G-3~~
~~Declassify On: X1~~

(U) **Enclosure(s):** ~~(S)~~ Original and one (1) copy of an LHM
concerning closing of above captioned case.

(S)

b1

~~SECRET/ORCON/NOFORN~~

~~SECRET~~/ORCON/NOFORN

To: Cyber From: Boston
(U) Re: ~~DS~~ 288B-BS-90939, 4/11/2003

(S)

[Redacted]

(S)

[Redacted]
No positive information was obtained.

b1

~~SECRET~~/ORCON/NOFORN

~~SECRET/ORCON/NOFORN~~

(U) To: Cyber From: Boston
Re: ~~(S)~~ 288B-BS-90939, 4/11/2003

LEAD(s):

Set Lead 1: (Info)

CYBER

AT WASHINGTON, DC

(U) Read and clear.

Set Lead 2: (Info)

GENERAL COUNSEL

AT WASHINGTON, DC

(U) Read and clear.

Set Lead 3: (Info)

BOSTON

AT BOSTON

(U) Read and clear.

♦♦

~~SECRET/ORCON/NOFORN~~

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY

Date: 07/23/2003

To: Counterterrorism

Attn: ITOS 1/CONUS 2/ TEAM 6

SSA [REDACTED]

IOS [REDACTED]

TFOS [REDACTED]

SC [REDACTED]

Cyber

Attn: SSA [REDACTED]

CIS/C3IU

Boston

Attn: ASAC [REDACTED]

SSA [REDACTED]

From: Boston

CT-3

Contact: SA [REDACTED]

b6
b7C

Approved By: [REDACTED]

Drafted By: [REDACTED]

dd

Case ID #: (S) [REDACTED]

CLASS (Pending)

(U)

(S) 288B-BS-90939 (Closed)

(S) 288B-HQ-1394667 (Closed)

b7A

Title: (S) [REDACTED]

(U)

dba, PTECH, INC.,
Quincy, Massachusetts;
AOT - IT - WCC

Synopsis: (U) Notify TFOS and CYBER of recent information provided to Boston by the Bureau of Customs and Immigration Enforcement (BICE).

(U)

~~Classified By: 2923, CT-3/Boston~~
~~Reason: 1.5(c)~~
~~Declassify On: X1~~

Details: (U) On July 23, 2003, SSA [REDACTED] BICE, Boston advised FBI Boston of recent information proffered to BICE, by the United States Secret Service (USSS), Washington, D.C. BICE Boston advised that apparently Senator Charles Grassley's Office requested that USSS, Department of Homeland Security conduct an independent review of the software sold by PTECH of Quincy, Massachusetts in order to determine if it represented a potential

~~SECRET~~

~~SECRET~~

To: Counterterrorism From: Boston
(U) Re: ~~(S)~~ 265C-BS-90861-CLASS, 07/23/2003

infrastructure threat. PTECH's core software product is known as Framework. The software is a strategic planning software product. Boston has only limited information at this time, however, SSA [] BICE, Boston indicated that the USSS contracted with an unnamed independent contractor to review PTECH'S product. Apparently this independent contractor's analysis suggests that PTECH's product poses a potential threat to the US computer infrastructure. In addition, this contractor is suggesting that [] and [] at PTECH, may have duplicated hard drives of the clients he visited on behalf of PTECH, and then took these hard drives with him out of the country to Egypt.

b6
b7C

(U) The Assistant US Attorney in charge of the PTECH investigation in Boston is aware of these allegations and has advised SSA [] of BICE that the USSS must produce their source and the related report so that the Boston investigative team can evaluate the information and follow up on it.

(U) It should be noted that [] was recently interviewed during the course of this investigation while he was on a short visit to the Boston area. [] left Boston and is believed to be back in Egypt. There are indications that [] may be returning to the Boston area in August, 2003 for further interview and possible Federal Grand Jury testimony. Also, [] operates a software company in Egypt with his wife. The firm, known as HORIZONS, conducts software testing for PTECH. At the founding of PTECH in 1994, PTECH was assisted in obtaining funding by an entity known as BMI. One of the principals of BMI at that time was [] []

~~SECRET~~

~~SECRET~~

(U) To: Counterterrorism From: Boston
Re: ~~8~~ 265C-BS-90861-CLASS, 07/23/2003

LEAD(s) :

Set Lead 1: (Info)

COUNTERTERRORISM

AT ITOS 1/CONUS 2/TEAM 6

(U) Read and clear.

Set Lead 2: (Discretionary)

CYBER

AT CIS/C3IU

(U) Liaise with TFOS and Boston regarding appropriate response when additional details become available.

Set Lead 3: (Action)

COUNTERTERRORISM

AT TFOS

(U) Obtain additional details regarding recent information from BICE regarding USSS review of PTECH product through BICE, Deputy, [REDACTED], assigned to TFOS.

b6
b7c

(U) Through liaison with USSS in Washington, D.C., obtain details concerning the examination of PTECH software including any reports generated with the identity of any experts utilized in this process.

♦♦

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 08/14/2003

To: Boston

Attn: SSA [redacted]
SSA [redacted]
SA [redacted]
SA [redacted]
SA [redacted]

From: Boston

CT-3

Contact: SA [redacted]

b6
b7C

Approved By: [redacted]

Drafted By: [redacted]

dd

Case ID #: [redacted]

(Pending)
199N-BS-86451 (Pending)
199N-BS-86457 (Pending)
288B-BS-90939 (Closed)

b7A

Title: [redacted]

dba, PTECH, INC.,
Quincy, Massachusetts'

Synopsis: Provide work product of CERT Coordination Center regarding their examination of PTECH, INC. software and overview of their contents.

Enclosure(s): One letter undated to Senator Charles Grassley. One white paper entitled; "Possible Terrorist Links to Ptech, Inc., a U.S. Company".

Details: On July 23, 2003, Boston was advised by SSA [redacted] Bureau of Customs and Immigration and Enforcement that the United States Secret Service (USSS) had hired a third party to review the software produced by PTECH of Quincy, Massachusetts and that allegedly, the results of the review indicated that there was an U.S. infrastructure weakness related to the software. At the time only a small number of details were available, they did not include who had conducted the review and the results of the review. Additionally, it was indicated the USSS was not inclined to share the results with BICE, and by extension, the criminal investigative team involved in captioned case.

Since, that time, efforts have been made on various fronts to obtain more information from the USSS. On August 14, 2003, SSA [redacted] Cyber Division successfully obtained both referenced

To: Boston From: Boston
Re: 265C-BS-90861, 08/14/2003

enclosures. Through [redacted] efforts, it was learned that the third party review of PTECH's software was conducted by the CERT Coordination Center. CERT is the Computer Emergency Response Team located at the Software Engineering Institute at Carnegie Mellon University in Pittsburgh, Pennsylvania. CERT is a federally funded entity.

b6
b7C

The first enclosure, the undated to Senator Charles Grassley summarizes CERT's findings as it relates to their review of PTECH's software. According to [redacted] the letter was mailed to Senator Grassley on August 13, 2003. In CERT's letter to the Senator, it is clear that CERT was tasked with determining whether or not the software contained malicious code or "back doors" that may disclose an organization's sensitive information to outsiders. CERT's evaluation found no evidence of backdoors or other malicious code. Further CERT did not believe that further technical analysis of the software would yield new insights. It should be noted that CERT did opine that if PTECH were interested in gaining a detailed understanding of its client's operations, it would not need to install backdoors on its software. This opinion is based on CERT's assessment that because as they cite, "According to the whistleblower [redacted], it was common practice for the consultants to take copies of the resulting databases back to their office to perform additional work."

FIELD COMMENT: It is useful to note that with respect to CERT's last assessment, no definitive evidence has been found to date to indicate that anyone from PTECH's improperly collected proprietary or sensitive data from a client and brought it back to PTECH, and then further transferred outside of PTECH to unauthorized individuals. CERT's commentary in this area appears to be based on [redacted] interaction with [redacted] while [redacted] was working with her at JP MORGAN CHASE in 2002. [redacted] chief complaint on 05/22/2002 was that [redacted] and [redacted] at Ptech arrived at JP MORGAN with a laptop computer which he wanted to connect into the JP MORGAN computer network. According to [redacted] the traditional method is to bring diskettes for such an evaluation, and [redacted] was not allowed to connect his laptop into the JP MORGAN computer network for fear that he would download proprietary information into his laptop. [redacted] felt that there was a good possibility that [redacted] conducted this scam with other potential customers, but she had no proof. In [redacted] own words, over 14 months ago, she was not able to state that [redacted] had actually done anything wrong or committed any crime. Yet she was able to speculate that there was a good possibility that he conducted a scam with other PTECH clients without evidence of any kind. It is further worth pointing out that during the course of the captioned investigation, witnesses have been asked whether they were aware of any unauthorized handling of client data. There have been no responses suggesting a situation like that occurred.

To: Boston From: Boston
Re: 265C-BS-90861, 08/14/2003

The second enclosure, the white paper entitled; "Possible Terrorist Links to Ptech, Inc., a U.S. Company" was prepared by CERT as well. It appears to be prepared primarily based on information from [redacted] and information available from public sources. Generally, the information in the paper is well known to Boston. However, CERT's conclusions are significantly overstated, many lack any credible evidence to support them. In fact, the conclusions should more aptly be described as sheer speculation on the part of CERT.

The writer recommends all receiving parties closely review both documents.

b6
b7C

SSA [redacted] assessment was that the conclusions by CERT were not substantially different from CYBER's original assessment that there was no evidence of backdoors or malicious code within the software.

Both documents have been made available to Assistant US Attorney [redacted] and SA [redacted] BICE. Furthermore, SSA [redacted] has provided copies of the documents to ITOS 1/CONUS 2/TEAM 6 and TFOS.

Boston's investigation continues.

♦♦

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 09/3/2003

To: Boston

Attn: SSA [redacted] (CT-3)

SA [redacted] (CT-3)

SA [redacted] (CT-1)

Counterterrorism

Attn: SSA [redacted]
CONUS II/ITOS 1 room 5270
SC [redacted]

Office of Public Affairs

Attn: SSA [redacted]
TFOS room 4871
Congressional Affairs Office
Room 7240

b6
b7c

From: Cyber

CIS/C3IU/room 5931

Contact: SSA [redacted]

Approved By: [redacted]

Drafted By: [redacted]

asm

Case ID #: (S) [redacted] CLASS (Pending)

(U) (S) 288B-BS-90939 (Closed)

(S) 288B-HQ-1394667 (Closed)

b7A

(U) **Title:** ~~(S)~~ [redacted]

DBA, PTECH, INC.,
QUINCY, MASS.
AOT - IT - WCC

(U) **Synopsis:** ~~(S)~~ To provide receiving offices with (1) a copy of a White Paper regarding PTECH Inc., and (2) a letter addressed to Senator Charles Grassley, both prepared by Carnegie Mellon University CERT (computer incident response team).

(U) ~~(S)~~

Derived From : G-3
Declassify On: ~~X1~~

(U) **Enclosures:** ~~(S)~~ Enclosed for receiving offices is one (1) copy of a document entitled, "White Paper: Possible Terrorist Links To Ptech, Inc., a U.S. Company", prepared by Carnegie Mellon CERT, and (2) copy of a letter addressed to Senator Grassley from Carnegie Mellon CERT (not dated).

~~SECRET~~

~~SECRET~~

To: Boston From: Cyber
(U) Re: ~~(S)~~ [REDACTED] -CLASS, 09/3/2003

b7A

Details: (U) Reference Boston EC to Counterterrorism dated 7/23/2003, and telcalls between SSA [REDACTED] C3IU/CyD, SA [REDACTED] Boston, and SSA [REDACTED] ITOS/CTD.

b6
b7C

(U) ~~(S)~~ For the information of receiving offices, on 8/12/2003, A/SC [REDACTED] (U.S. Secret Service detailee to the Cyber Division, FBIHQ), Computer Intrusion Section (CIS), obtained the enclosed White Paper from the USSS congressional affairs office, Washington D.C. A/SC [REDACTED] advised that the document was prepared by the CERT, Carnegie Mellon University, Pittsburgh, PA. pursuant to a request from Senator Charles Grassley's office thru USSS. He advised that CERT was requested to conduct technical analysis of Ptech software in connection with Senator Grassley's inquiries into the possible threat posed by Ptech and its product/services due to its alleged connections to terrorist groups and individuals. He advised that Senator Grassley's office staff may be requesting a meeting with the FBI once the CERT reports are completed and provided to the FBI for review.

(U) ~~(S)~~ On 8/13/2003, through Cyber Division/CCIU and Pittsburgh Division liaison with Carnegie Mellon CERT, CERT provided a copy of a letter addressed to Senator Grassley from CERT. The letter was pursuant to Senator Grassley's request for the CERT to examine Ptech Inc. software for evidence of malicious code or "back doors." The letter also provided CERT's conclusions which in essence stated that the CERT's evaluation found no evidence of backdoors or other malicious code and that "further evaluation of the software will not yield new insights." CERT advise that the letter was forwarded

(U) In view of the above, C3IU/CyD will consider the referenced lead completed.

LEAD (S) :

~~SECRET~~

~~SECRET~~

(U) To: Boston From: Cyber
Re: ~~(S)~~ [REDACTED] CLASS, 09/3/2003

b7A

Set Lead 1: (Info)

BOSTON DIVISION

AT BOSTON, MASSACHUSETTS

(U) Read and clear.

Set Lead 2: (Info)

COUNTERTERRORISM

AT WASHINGTON D.C.

(U) Read and clear.

Set Lead 3: (Info)

OFFICE OF PUBLIC AFFAIRS

AT WASHINGTON D.C.

(U) Read and clear.

~~SECRET~~

~~SECRET~~

To: Boston From: Cyber
(U) Re: ~~S~~ 265C-BS-90861-CLASS, 09/3/2003

Set Lead 1: (Info)

BOSTON DIVISION

AT BOSTON, MASSACHUSETTS

(U) Read and clear.

Set Lead 2: (Info)

COUNTERTERRORISM

AT WASHINGTON D.C.

(U) Read and clear.

Set Lead 3: (Info)

OFFICE OF PUBLIC AFFAIRS

AT WASHINGTON D.C.

(U) Read and clear.

~~SECRET~~

~~SECRET~~

04/11/03
10:12:30

Lead Upload Report

ICMLPE11
Page 1

Case ID: 288B-HQ-1394667
Serial: 6

*** WARNING ***
*** WARNING ***

City name invalid
City isn't covered by the office which the lead is

~~SECRET/NOFORN/ORCON~~

DATE: 06-22-2011
FBI INFO.
CLASSIFIED BY 60324 UCBAW/SAB/SBS
REASON: 1.4 (c)
DECLASSIFY ON: 06-22-2036



U.S. Department of Justice

Federal Bureau of Investigation

Washington, D C 20535-0001

October 28, 2002

(U) ~~SECRET~~ PTECH INC. - SUBJECT (U.S. COMPANY);
FBI, FAA, IRS, USAF, DOE, OTHER U.S. GOVERNMENT AGENCIES -
POSSIBLE VICTIMS;
TARGETING THE NATIONAL INFORMATION INFRASTRUCTURE -
COUNTERINTELLIGENCE/COUNTERTERRORISM (TNII-CI/CT)
FILE #288B-HQ-1394667

(U) Full Field Investigation instituted: 8/23/2002

(U) ~~SECRET~~ Derived From: G-3
Declassify On: X-1

(U) ~~SECRET~~ Since June 1995, the Boston FBI Counterterrorism
(CT) squads have been investigating several individuals who
have had numerous contacts and associations with persons and
groups suspected of ties to international terrorism. Some of
these individuals include [REDACTED]

[REDACTED] and [REDACTED]
[REDACTED] and [REDACTED] are associated, as
described below, with Ptech Inc. (Ptech), Quincy,
Massachusetts, a computer software company. Source reporting
and the Ptech Internet website have listed the FBI, FAA, IRS,
USAF, DOE, and other U.S. government agencies as Ptech
customers. Source information has also reported that Ptech
may have done business with the White House and/or the Vice
President's office, under the auspices of another company
named Process Renewal Group (PRG).

(U) Ptech Inc. is a business involved in providing
enterprise architecture and business modeling, analysis and
integration solutions to Global 2000 companies. This
technology addresses every aspect of the organization, from
strategic planning, to business architecture; from business
processes to network, supporting applications, and all forms
of information, which is integrated to form a complete
representation of the company's knowledge. Massachusetts
State corporate records list Ptech Inc. as a partnership, its
business address as 160 Federal Street, Boston, MA. 02110, and
its [REDACTED] and [REDACTED] as [REDACTED]

[REDACTED] The records further references
an involuntary dissolution date of 8/31/1998, and a subsequent

~~SECRET/NOFORN/ORCON~~

288B-HQ-1394667-4

b6
b7C

~~SECRET/NOFORN/ORCON~~

revival date of 6/1/2001. Lexis/Nexis checks of Ptech list the company's other principals as [redacted] and [redacted]

b6
b7c

(U) ~~(S)~~ On 6/27/1995, FBI Boston opened a preliminary inquiry (PI) on [redacted] based on his telephone contacts with the Holy Land Foundation for Relief and Development (HLFRD), Dallas, Texas. HLFRD is an organization suspected of being a source for funding terrorist activities and groups.

(U) ~~(S)~~ (NF/OC) Investigation of [redacted] had also revealed that he had telephone contacts with [redacted] subjects and was associated with other Boston international terrorism subjects. A Full Field Investigation (FFI) (199N-BS-77139) was initiated by FBI Boston on 6/11/2002.

(U) ~~(S)~~ Source information has indicated that [redacted] and other Ptech employees traveled to Saudi Arabia, during February 1999, to seek funding from a wealthy Saudi Arabian name [redacted]. Sources have also reported that [redacted] may have been the source of approximately \$16 million in startup funds for Ptech. [redacted] has been described as one of the "chief money launderers" for OSAMA BIN LADEN.

(U) ~~(S)~~ Source reporting has indicated that another individual, [redacted] is associated with [redacted] and Ptech. [redacted] is reported to be a Pakistani National on the Ptech Board of Directors. [redacted] is also the head of SAAR Foundation, Herndon, VA. This foundation has been linked to financial organizations that are being investigated for handling large sums of money to fund activities for OSAMA BIN LADEN and various other terrorist organizations. SAAR is the subject of a U.S. Customs Service (USCS)/Joint Terrorism Task Force (JTTF) case. [redacted] is a central figure in this investigation. Searches of the offices of SAAR Foundation, and other foundations in the Northern Virginia area, were conducted by federal agents during March 2002, in connection with the USCS/JTTF investigation.

(S) ~~(S)~~ (NF/OC) [redacted] a U.S. person, is employed as a computer software engineer for Ptech. [redacted] also serves as the current president and as a long-time member of CARE INTERNATIONAL, a non-governmental organization in Boston with ties to international terrorism and as a source of funding for terrorist activities. [redacted] is the subject of a FBI Boston FFI (199N-BS-86457). [redacted]

b1

~~SECRET/NOFORN/ORCON~~

~~SECRET/NOFORN/ORCON~~

(S) [REDACTED] This investigation has revealed that CARE INTERNATIONAL serves as a front for recruiting local Muslims to participate in international jihad effort.

b1

(U) ~~(S/NF/OC)~~ [REDACTED] is an employee of Ptech Inc., in Boston, and is the [REDACTED] and [REDACTED] of Care International, a non-governmental organization in Boston with ties to international terrorism. Care International was previously known as the Al-Kifah Refugee Center of Boston. Following the World Trade Center attack in 1993, Al-Kifah changed its name to Care International after the media reported that members of the Al-Kifah Refugee Center of New York were involved in the attack. In the Boston area, Care International has served as a front for recruiting/funding local Muslims to participate in the international Jihad efforts. [REDACTED] is closely associated with [REDACTED] the [REDACTED] of Care International.

b6
b7C

(U) ~~(S)~~ On May 28, 2002, a complainant working for JP Morgan Chase in Manhattan, NY, reported suspicious business practices by Ptech. This complainant was concerned that Ptech was involved in the theft of technology from U.S. companies. This complainant advised that [REDACTED] is connected to organizations which provide funding for terrorist purposes. This complainant further indicated that a Ptech employee may have tried to gain access to the Chase network during a demonstration of Ptech products and/or services, although there is no independent information to corroborate this.

(U) ~~(S)~~ On August 23, 2002, it was determined that the Information Resources Management (IRM) Office, FBIHQ, had purchased Enterprise Architecture computer software from Ptech in early 2001. This software, named "Framework," was being used as a management tool on the FBI's intranet network and is used for the FBI Enterprise Architecture project. The software allows users to access the FBI's Strategic Plan, organization chart, business processes, and other applications.

(U) ~~(S)~~ Ptech Framework software originals and copies including updated versions and "accelerators" were provided to the Counterintelligence Counterterrorism Computer Intrusion Unit (C3IU), Cyber Division, by IRM for technical analysis. Preliminary technical analysis of the Ptech software by the Special Technologies and Applications Unit (STAU) to date has not revealed any evidence of malicious (eg. trojans,

~~SECRET/NOFORN/ORCON~~

~~SECRET/NOFORN/ORCON~~

backdoors, viruses, worms, etc.) or any other unauthorized code imbedded in the software. Examination of two IRM computers used to run the software has not revealed any abnormalities. According to IRM, the Ptech software was not used to connect to the FBI computer network. Referral/Consult

(S)

- (U) ~~(S)~~ IRM personnel (section chief, chief architect, computer scientist, contractors) who worked with the Ptech software on the FBI Enterprise Architecture project have been interviewed. These individuals had no direct contacts or dealings with Ptech or its personnel with the exception of receiving training from instructors from Ptech. The reason is that the Ptech software purchased by the FBI was actually purchased through a government contractor called SPAWAR (Space and Naval Warfare).
- (U) ~~(S)~~ C3IU has obtained documents from IRM and the Contracts Unit that relate to the FBI purchase of the Ptech software. The documents indicate that during 12/2001, the FBI purchased two licensed copies of the Ptech Framework software, including updates and accelerators, for use in developing the FBI's Enterprise Architecture (EA) at a cost of \$15,000. The purchase was actually made by SPAWAR on behalf of the FBI and pursuant to the SPAWAR contract.
- (U) ~~(S)~~ The FBI New York Cyber squad has advised that they have been working with the security department of JP Morgan Chase Bank, NY, concerning Ptech's efforts to market their software to the bank. JP Morgan security advised that a Ptech representative was allowed limited access to the company's network for this purpose. JP Morgan Chase Bank security conducted a thorough search of all areas of their network accessed by the Ptech representative but did not find any abnormalities. They advised that during a Ptech software demonstration at JP Morgan Bank, JP Morgan denied the Ptech's representative's request to connect his computer with the company's network. As a result of the above dealings with Ptech, JP Morgan did not purchase software from the company.

~~SECRET/NOFORN/ORCON~~

~~SECRET/NOFORN/ORCON~~

(U) ~~(S)~~ Source information and public records have indicated that the Process Renewal Group (PRG) is a consulting group out of Vancouver, British Columbia, Canada. A former Ptech Inc. employee, [REDACTED] was once employed by PRG. Source information has further indicated that PRG never had a contract with the White House as has been claimed by Ptech advertisements and is believed to be fabricated by [REDACTED] and others for the benefit of Ptech. The Contracts Unit, Finance Division, FBIHQ, advised that they failed to locate any records of doing business with PRG.

b6
b7C

(S) ~~(S)~~ The FBI Boston's counterterrorism investigation to date [REDACTED] [REDACTED] has not developed any information or indications that Ptech has been involved in the installation of any malicious or unauthorized code or backdoors into the FBI or other government networks, either through their software or services.

b1

(U) ~~(S)~~ The FBI Boston Division Cyber squad has been working closely with the Boston Counterterrorism squads to coordinate the investigations of Ptech and its principals. Boston's Cyber squad in conjunction with FBIHQ, will evaluate the extent and nature of the threat to the national information infrastructure posed by Ptech Inc. and its principals and employees.

(S)

b1

~~SECRET/NOFORN/ORCON~~

~~SECRET/NOFORN/ORCON~~

(S)

(S)

No positive information was discovered.

b1

No positive information was obtained.

No positive information was obtained.

(U) ~~(S)~~ IRM conducted a canvass of all FBI divisions to determine if any other Ptech products were being used or had been acquired. The results of the canvass determined that no one else in the FBI reported acquiring or using any Ptech products. IRM and the FBI has discontinued the use of the Ptech Framework software and a decision has been made not to acquire or use Ptech products in the future.

(S)

The specific purpose of these interviews would be to obtain information concerning Ptech's involvement in planting malicious code or unauthorized code in their software or efforts to implant them in U.S. computer networks.

Referral/Consult

(U) Investigation continuing.

~~SECRET/NOFORN/ORCON~~

~~SECRET/ORCON/NOFORN~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 08/24/2002

To: Counterterrorism
Boston

Attn: SSA [redacted] - UBLU
SSA [redacted]

From: Cyber Division
C3IU/CIS/#5931
Contact: SSA [redacted]

b6
b7C

Approved By: [redacted]

Drafted By: [redacted] asm

(U) Case ID #: ~~(S)~~ 288B-NEW (Pending)

(U) Title: ~~(S)~~ PTECH INC - SUBJECT (A U.S. COMPANY);
FBI, FAA, IRS, USAF, DOE, OTHER U.S.
GOVERNMENT AGENCIES - POSSIBLE VICTIMS
TARGETING THE NATIONAL INFORMATION
INFRASTRUCTURE - COUNTERINTELLIGENCE/
COUNTERTERRORISM (TNII-CI/CT)
OO.HQ

(U) Synopsis: ~~(S)~~ Initiation of Full Field Investigation (FFI) on
captioned matter.

(U) ~~(S)~~ Derived From: G-3
Declassify On: ~~X1~~

(U) ~~(S)~~ Full Field Investigation Instituted: 8/23/2002

(U) Details: ~~(S)~~ Since June 1995, the Boston FBI counterterrorism
squads have been investigating several individuals who have had
numerous contacts and associations with persons and groups
suspected of ties to international terrorism. Some of these
individuals include [redacted]
[redacted] and [redacted] and [redacted] are
associated, as described below, with Ptech Inc. (Ptech), Quincy,
Massachusetts, a computer software company. Source reporting and
the Ptech Internet website have listed the FBI, FAA, IRS, USAF,
DOE, and other U.S. government agencies as Ptech customers. Source

~~SECRET/ORCON/NOFORN~~

288B-HQ -1394667-1

~~SECRET/ORCON/NOFORN~~

(U) To: Counterterrorism From: Cyber Division
Re: ~~S~~ 288B-NEW, 08/24/2002

information has also reported that Ptech may have done business with the White House and/or the Vice President's office, under the auspices of another company named Process Renewal Group (PRG).

(U) ~~S~~ Corporate records list [] as the [] and [] for Ptech. According to these records, [] established Ptech in 1994. He has been described as the [] and [] behind this entity.

b6
b7C

(U) ~~S~~ On 6/27/1995, FBI Boston opened a preliminary inquiry (PI) on [] based on his telephone contacts with the Holy Land Foundation for Relief and Development (HLFRD), Dallas, Texas. HLFRD is an organization suspected of being a source for funding terrorist activities and groups.

(U) ~~S/NF/OC~~ Investigation of [] had also revealed that he had telephone contacts with HAMAS subjects and was associated with other Boston international terrorism subjects. A Full Field Investigation (FFI) (199N-BS-77139) was initiated by FBI Boston on 6/11/2002.

(U) ~~S~~ Source information has indicated that [] and other Ptech employees traveled to Saudi Arabia, during February 1999, to seek funding from a wealthy Saudi Arabian name [] aka []. Sources have also reported that [] may have been the source of approximately \$16 million in startup funds for Ptech. [] has been described as one of the "chief money launderers" for OSAMA BIN LADEN.

(U) ~~S~~ Source reporting has indicated that another individual, [] is associated with [] and Ptech. [] is reported to be a Pakistani National on the Ptech Board of Directors. [] is also the [] SAAR Foundation, Herndon, VA. This foundation has been linked to financial organizations that are being investigated for handling large sums of money to fund activities for OSAMA BIN LADEN and various other terrorist organizations. SAAR is the subject of a U.S. Customs Service (USCS)/Joint Terrorism Task Force (JTTF) case. [] is a central figure in this investigation. Searches of the offices of SAAR Foundation, and other foundations in the Northern Virginia area, were conducted by federal agents during March 2002, in connection with the USCS/JTTF investigation.

~~S/NF/OC~~ [] a U.S. person, is employed as a computer software engineer for Ptech. [] also serves as the current [] and as a long-time member of CARE

~~SECRET/ORCON/NOFORN~~

~~SECRET~~/ORCON/NOFORN

(U) To: Counterterrorism From: Cyber Division
Re: ~~SECRET~~ 288B-NEW, 08/24/2002

INTERNATIONAL, a non-governmental organization in Boston with ties to international terrorism and as a source of funding for terrorist activities. [REDACTED] is the subject of a FBI Boston FFI (199N-BS-86457).

b6
b7C

(S) [REDACTED] This investigation has revealed that CARE INTERNATIONAL serves as a front for recruiting local Muslims to participate in international jihad efforts.

b1

(U) ~~SECRET~~ On August 23, 2002, Section Chief Mark Tanner, Information Resources Management (IRM) Office, FBIHQ, advised that the FBI had purchased Enterprise Architecture computer software from Ptech in early 2001. This software, named "Framework," is currently being used as a management tool on the FBI's intranet network and is used for the FBI Enterprise Architecture. The software allows users to access the FBI's Strategic Plan, organization chart, business processes, and other applications.

(U) ~~SECRET~~ The Cyber Division is working with the IRM Office to conduct a thorough technical analysis of the Ptech software to determine if the software poses a threat to the FBI network or can be utilized to install a backdoor for later access. The analysis is a two pronged approach. First, an analysis of the software computer compact discs to determine if the software installed any malicious or unauthorized code into the FBI networks, or provides a backdoor to these networks. As of 8/24/2002, preliminary technical analysis of the compact discs conducted by Crucial Security, Special Technology and Applications Unit (STAU), has not revealed any abnormalities. The second phase is to monitor, at the network level, the computer server where the Ptech software currently resides, to look for any anomalous activity of that server with the FBI networks. Crucial Security is currently conducting this type of analysis.

(S) [REDACTED]

(S) While this analysis of the software and the server's relationship with the FBI network is being conducted, efforts are ongoing to fully identify all government customers of Ptech.

Referral/Consult

~~SECRET~~/ORCON/NOFORN

~~SECRET/ORCON/NOFORN~~

(U) To: Counterterrorism From: Cyber Division
Re: ~~(S)~~ 288B-NEW, 08/24/2002

(U) ~~(S)~~ On May 28, 2002, a complainant working for JP Morgan Chase in Manhattan, NY, reported suspicious business practices by Ptech. This complainant was concerned that Ptech was involved in the theft of technology from U.S. companies. This complainant advised that [redacted] is connected to organizations which provide funding for terrorist purposes. This complainant further indicated that a Ptech employee may have tried to gain access to the Chase network during a demonstration of Ptech products and/or services, although there is no independent information to corroborate this.

b6
b7C

(S) ~~(S)~~ The FBI Boston's counterterrorism investigation to date, [redacted] has not developed any information or indications that Ptech has been involved in the installation of any malicious or unauthorized code or backdoors into the FBI or other government networks, either through their software or services.

b1

(U) ~~(S)~~ The FBI Boston Division Cyber squad has been working closely with the Boston Counterterrorism squads to coordinate the investigations of Ptech and its principals. Boston's Cyber squad in conjunction with FBIHQ, will evaluate the extent and nature of the threat to the national information infrastructure posed by Ptech Inc. and its principals and employees.

~~SECRET/ORCON/NOFORN~~

~~SECRET/ORCON/NOFORN~~

(U) To: Counterterrorism From: Cyber Division
Re: ~~(S)~~ 288B-NEW, 08/24/2002

LEAD(s):

Set Lead 1:

COUNTERTERRORISM

AT WASHINGTON, DC

(U) ~~(S)~~ UBL Unit is requested to continue close coordination with the Cyber Division/C3IU concerning parallel 199N/288B matters regarding Ptech Inc and it's principals and employees. The Cyber Division's main focus will be to thoroughly investigate Ptech Inc. and individuals associated with the company including its principals and employees, who may be involved in designing and modifying software and/or performing services for the purpose of compromising the networks of their government and non-government customers.

Set Lead 2:

BOSTON

AT BOSTON, MASSACHUSETTS

(U) ~~(S)~~ Boston Division's Cyber (NIPCIP) Squad is requested to initiate a separate 288B matter, and continue to coordinate investigations with CT-1 squad (SSA).

b6
b7C

♦♦

~~SECRET/ORCON/NOFORN~~